The Zero Trust eXtended (ZTX) Ecosystem

Extending Zero Trust Security Across Your Digital Business

by Chase Cunningham

January 19, 2018

Why Read This Report

Security pros are still scrambling for new and effective ways to protect their networks and combat the impacts of hacking and exploitation. With Forrester's Zero Trust Model of information security, you can develop robust prevention, detection, and incident response capabilities to protect your company's vital digital business ecosystem. This report will help security pros understand the technologies best suited to empowering and extending their Zero Trust initiatives and will detail how Forrester sees this model and framework growing and evolving.

Key Takeaways

Zero Trust Platforms Are Emerging

The days of cobbling together disparate technologies to protect and secure the network are going the way of the dinosaur. Major security vendors are building powerful platforms focused on enabling Zero Trust strategies. Choosing which platform to use is vital in your Zero Trust planning.

Strategy Must Drive The Technology

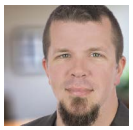
In many other areas, technology capabilities compose the crux of selection criteria. However, to achieve a Zero Trust network, strategy is more critical than the technology will ever be. Your strategy should always drive the technology selection.

No API, Look Elsewhere

Any vendor or technology worth their salt will have advanced API integration available for your team to use for development purposes as well as to integrate other security solutions into your Zero Trust ecosystem. If your selected technology doesn't have solid APIs to use, find another vendor that does.

The Zero Trust eXtended (ZTX) Ecosystem

Extending Zero Trust Security Across Your Digital Business



by Chase Cunningham
with Stephanie Balaouras, Bill Barringham, and Peggy Dostie

January 19, 2018

Table Of Contents

Related Research Documents

Develop Your Zero Trust Workforce Security Strategy

Five Steps To A Zero Trust Network

Future-Proof Your Digital Business With Zero Trust Security

FORRESTER®

Forrester Research, Inc., 60 Acorn Park Drive, Cambridge, MA 02140 USA
+1 617-613-6000 | Fax: +1 617-613-5000 | forrester.com

Zero Trust Has Become A Driving Force In Cybersecurity

If the news of the past six months is any indication of the current security state of most networks, our industry is in a perfect circle of failure.[1] The malicious actors of the world spend their time looking for the overt and easy targets without fear, and those accesses and compromise vectors are working with great success. This is despite a decade or more of subject matter experts espousing the need for better security controls. While this is the sad reality for a large swath of the world's networks, those security teams that have embraced Zero Trust don't wind up in the headlines. Zero Trust can't prevent every possible attack or breach, but it can ensure that organizations don't fall victim to the easiest of attacks or fail to discover a breach for months or even years.

At its simplest, Forrester's Zero Trust Model of information security is a conceptual and architectural model for how security teams should redesign networks into secure microperimeters, strengthen data security using obfuscation techniques, limit the risks associated with excessive user privileges and access, and dramatically improve security detection and response with analytics and automation. Security teams across the globe are adopting these concepts and strategies because Zero Trust:

- **Protects the business from advanced threats and the impacts of breaches.** When cybercriminals exfiltrate intellectual property, such as designs, formulas, road maps, and corporate strategy, it can lead to millions in lost revenues, and, if competitors bring cheaper knock-offs to market, even a permanent erasure of competitive advantage.[2] When they exfiltrate sensitive customer data, it can lead to millions in breach response and remediation costs, years of lawsuits and regulatory investigations, and damage to the firm's brand for the foreseeable future. Visibility is the key in defending any valuable asset. You can't protect the invisible. The more visibility you have into your network across your business ecosystem, the better chance you have to quickly detect the tell-tale signs of a breach in progress and to stop it.[3] Zero Trust mandates significant investment in visibility and analytics across the business — regardless of location or hosting model.[4]
- **Easily supports new business and operational models.** In many instances, securing a system, network, or infrastructure is a complicated endeavor. This is even truer for today, as businesses rapidly adopt new cloud services, create new customer engagement models, and continue to expand employee bring-your-own-anything policies. Our perimeters and boundaries have been obliterated. Using a Zero Trust approach, these same challenges are turned into power points. Virtualization, microsegmentation, and granular data control strategies are key elements of a Zero Trust strategy; thanks to their conceptual simplicity, the need for their use is apparent and visible for everyone at the organization.[5]
- **Enables compliance.** Almost any business that touches the internet today has a compliance requirement such as FISMA, HIPAA, and PCI. For many compliance requirements and audits, having a secure, segmented network is a basic tenet. Security teams that have used Zero Trust as a key driver of their strategic security vision have met many compliance requirements with far greater ease. This is because segmenting your network frequently reduces the scope of

compliance initiatives because many regulations, such as PCI, only have certain data types in scope.[6] In fact, Zero Trust networks far exceeded the security required by compliance directives, and that's a good thing.

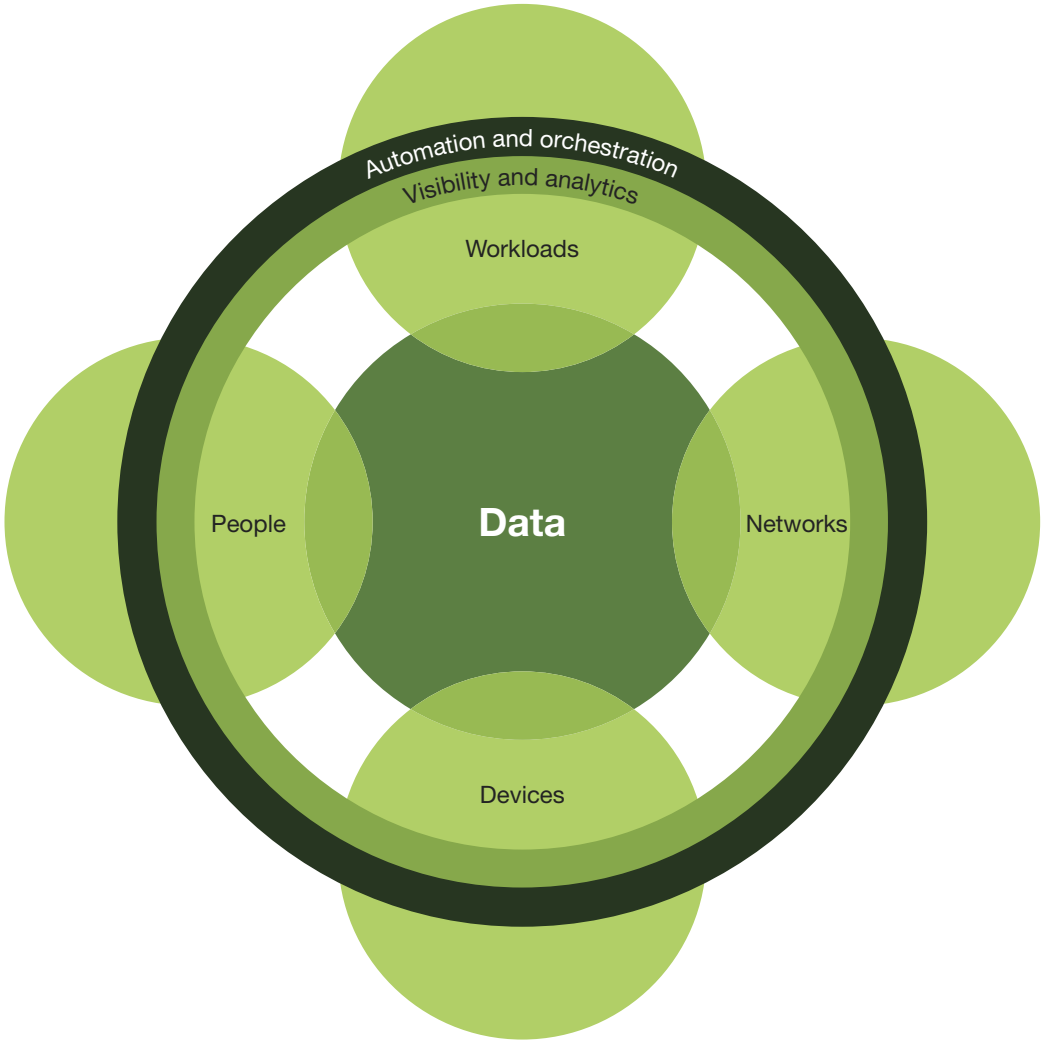
Zero Trust Extends Across The Entire Digital Ecosystem

Originally, the driving force behind Zero Trust was a need to move security pros away from a failed perimeter-centric approach to security to a model that was much more data- and identity-centric and better adapted for today's digital business, where even the most basic business processes are rarely self-contained within the four walls of the corporation. Initially, we spent a great deal of time explaining the value of breaking down monolithic perimeters into a series of microperimeters or network segments where security pros could concentrate granular security controls as well as contain attacks. Over time, security pros came to associate Zero Trust primarily with network segmentation and the obvious vehicle for enforcing that segmentation, the next-generation firewall (NGFW).[7] But Zero Trust is more than network segmentation; it's a complete and holistic approach that includes processes and technologies for:

- **Zero Trust data.** One of the pillars of a Zero Trust strategy is data security, which is ultimately a technology solution. Securing and managing the data, categorizing and developing data classification schemas, and encrypting data both at rest and in transit are key pieces of any Zero Trust approach. A variety of vendors have realized this and have begun to invest heavily in enabling these strategic initiatives within their Zero Trust technology stacks and platforms: Cisco has UCS, and IBM has an extensive encryption portfolio. Other vendors focused in this specific arena offer technical solutions that merit your consideration when mapping out your team's Zero Trust plans.
- **Zero Trust networks.** The ability to segment, isolate, and control the network continues to be a pivotal point of control for Zero Trust. Vendors have realized the power that segmentation and isolation offer to better secure networks, and they have invested heavily in making their solutions in this space easy to use and powerful when leveraged by seasoned S&R pros. Cisco, Forcepoint, Palo Alto Networks, VMware, and others have rolled out technical features and network hooks that benefit Zero Trust initiatives and should be included in any S&R evaluation of Zero Trust network technologies.
- **Zero Trust people.** The last line of any Zero Trust strategy is limiting and strictly enforcing the access of users and securing those users as they interact with the internet.[8] This encompasses all the technologies necessary for authenticating users and continuously monitoring and governing their access and privileges.[9] It also encompasses the technologies for securing and protecting users' interactions like traditional web gateway solutions. A variety of new vendors have emerged that have built solutions that can help security pros do this in new ways. Authentic8, LightPoint, Menlo, and Symantec (FireGlass) all offer remote browser isolation technology that lets your team extend the defensive perimeter outward toward the internet and can help keep your workforce from becoming the first point of compromise as part of your Zero Trust strategy.[10]

- **Zero Trust workloads.** Workloads is a term that some security pros are unfamiliar with but that is standard for counterparts in infrastructure and operations.[11] It's a high-level term that refers to the entire application stack from the app layer through the hypervisor or self-contained components of processing such as containers and virtual machines within the stack. The workloads are the front-end and back-end systems that run the business and help it win, serve, and retain customers.[12] Just as with any other area of Zero Trust, these connections, apps, and components must be treated as a threat vector and must have Zero Trust controls and technologies applied to them. Of particular concern are workloads running in public clouds.
- **Zero Trust devices.** IoT and network-enabled device technologies have introduced a massive area of potential compromise for networks and enterprises.[13] Smart TVs, mobile devices, and even smart coffee makers are all over the market now, and each of those items introduces new avenues of code and assets that security teams must track and treat as untrusted in any infrastructure.[14] In order to really move toward a Zero Trust strategy, security teams must be able to isolate, secure, and control every device on the network at all times.[15]
- **Visibility and analytics.** You can't combat a threat you can't see or understand. Tools such as traditional security information management (SIM), more-advanced security analytics platforms, security user behavior analytics (SUBA), and other analytics systems enable security pros to know and comprehend what's taking place in the network. This focus area of the extended Zero Trust ecosystem helps with the ability of a tool, platform, or system to empower the security analyst to accurately observe threats that are present and orient defenses more intelligently.
- **Automation and orchestration.** Forrester has done extensive research and analysis in this area and has shown just how critical it is for organizations and S&R leadership to leverage and use tools and technologies that enable automation and orchestration across the enterprise.[16] The ability to have positive command and control of the many components that are used as part of the Zero Trust strategy is a vital piece of the extended Zero Trust ecosystem (see Figure 1).

FIGURE 1 Components Of The Zero Trust eXtended Ecosystem



The Zero Trust eXtended (ZTX) Ecosystem Framework

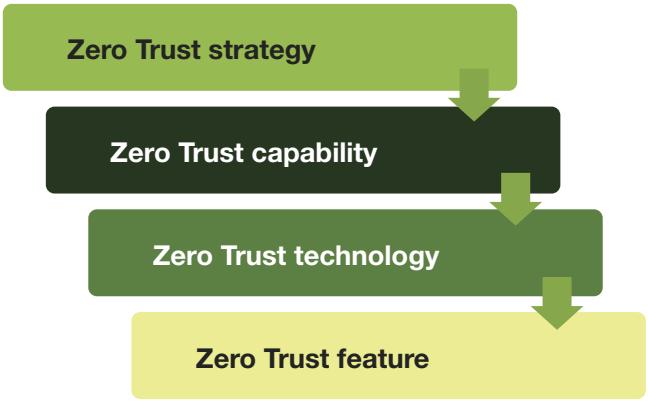
As with any well-built system, the Zero Trust ecosystem must grow and become more inclusive and prescriptive. To do this, Forrester has built a control mapping framework for the evolution of the Zero Trust ecosystem (see Figure 2). This more comprehensive view of Zero Trust provides security pros with a much more detailed reference point to determine specifically what tools and technologies are available in this space and precisely which they should leverage for their security operations needs:

› **Zero Trust strategy.** Your strategy is a high-level plan to achieve certain goals. It's what your organization strives toward. It's not a specific technology such as a next-generation firewall. Zero Trust is a strategic rally point for any team to better understand the clear and concise goal of

security in an operational context. Your team should understand the statement "Our goal is to evolve toward a Zero Trust network architecture" or "Our goal is to encrypt all sensitive data by default without undermining business use." Then they should all work to drive these strategic goals forward by adopting the other components of the framework. The strategy is to become a Zero Trust ecosystem, not buy a Zero Trust technology item and hope things are now "Zero Trust."

- **Zero Trust capability.** The Zero Trust ecosystem consists of several pillars or key components. Within these components are specific capabilities to achieve. For example, within data security, security teams need the ability to inventory, classify, obfuscate, archive, or delete data according to policy. Before you even consider a vendor or their technologies, you must understand the defined policies, processes, and procedures that you will need to underpin these capabilities. A vendor must be able to describe clearly what capabilities they offer within each component of the ecosystem — if they can't, it means they don't really understand Zero Trust and the very use of their tool or software could be a hindrance to achieving your Zero Trust strategic goals.
- **Zero Trust technology.** After you've articulated your strategic goals and identified the key capabilities you need to develop within each Zero Trust component, you're ready to consider a tool, software item, or platform that supports your Zero Trust strategy. As you evaluate technology, ask "What capabilities does this technology support and where does it specifically plug into my team's Zero Trust strategy?" Avoid point products that lack integration with the vendor's own solutions or with other heterogeneous solutions. For example, there are few vendors that offer data inventory, data flow mapping, data classification, data loss prevention, encryption, and data archiving in a single solution.[17] However, there are vendors that offer at least two of these capabilities with strong hooks between them and a strong partner ecosystem that can offer the rest, possibly with API integration support.
- **Zero Trust feature.** What is the specific feature of the technology that enables a capability to meet the Zero Trust strategy? This is the crux of this final and most granular point of this focused framework. Any vendor who claims to offer a Zero Trust-related solution must describe how the specific feature that they offer aligns with the other levels of the framework. For example, a DLP solution may have the ability to discover and classify data. Or a NFGW vendor may have a feature that allows an administrator to manage all firewalls on all networks from a single user interface (UI).

FIGURE 2 The Zero Trust eXtended Control Mapping Framework



Zero Trust Drives The Strategic Road Maps Of Security Vendors

Zero Trust demands that security teams retain visibility and control across their entire digital business ecosystem, regardless of location, device, user population, or hosting model. As a result, today's security vendors and providers have worked feverishly to improve their ease of use, breadth of capabilities and features, and integrations. Specifically, we have seen:

- **The emergence of powerful platforms.** The powerhouses in networking and operational security technology, like Cisco, IBM, and Palo Alto Networks, have all built powerful platform capabilities that integrate and leverage existing capabilities and features from across their broad portfolios for focused security operations. They are also serving as a platform to integrate with other heterogeneous security solutions. Consolidated offerings give security teams more visibility and control into their environment, and they also reduce the operational complexity and cost of managing individual point products. They also lay the foundation for automation and orchestration of security defenses.
- **The incorporation of security, data, and business context.** The failures that networks continue to experience originate from their inability to protect what matters — data. New platforms and solutions more easily integrate with data discovery and classification tools and other data sources that can help security teams better understand what data they really need to defend based on its classification and value to the business as well as whether there are known threats. The data is what matters, and the ability to not only understand its value but also where it lives and transits is best derived from platforms that are integrated and that increase security context around those valuable data stores.
- **A focus on ease of use.** Security leaders widely acknowledge that we have a human capital problem in security: 25% of global security decision makers say that staff shortages are a major challenge, and 22% say they lack staff with the right skills.[18] This problem is compounded when technologies aren't integrated and are disjointed operationally. Most of the new platforms under development

can improve security operations and empower security pros to be more operationally capable, as they offer advanced templates that improve the ease of use for network security configurations and simplify security controls into a single point of control and visibility. Most user interfaces within vendor solutions have dramatically changed and greatly improved visually from years past. Some of the more prevalent UIs of note are AlertLogic, Centrify, ForcePoint, and TrendMicro.

› **Integration of functionality across products from different security domains.** Usability and command and control of assets across disparate data systems, networks, and infrastructure are critical in Zero Trust. Platforms are becoming points of powerful integration and management capabilities, but you will still need to invest in point solutions. When you do, avoid solutions that function in isolation and opt for those that integrate to form an ecosystem to aid better visibility and control across the ecosystem and robust orchestration of security defenses. Vendors increasingly look for specific points of integration between one or more of their own products or with another vendor. This might be hooks between a vendor's own detection solutions and their authentication solutions or between a specialized automation vendor with a more traditional SIM or security analytics solution. Integration of these systems must be as seamless as possible to be considered part of the Zero Trust eXtended ecosystem.

Zero Trust Platform Vendors Provide Multiple Capabilities And Support API Integration

Major players in the market such as Cisco, IBM, and Palo Alto Networks have all begun to integrate technical components into platforms that underpin Zero Trust concepts. Security pros can expect other platform vendors to emerge. However, many vendors will claim to have a platform when in reality they have a loosely coupled portfolio of independent point products. In order to be a Zero Trust platform, a security vendor or provider must:

› **Offer market-leading capabilities in at least three Zero Trust components.** In order to be a strategic Zero Trust player, a vendor or provider must offer at least three market-leading Zero Trust capabilities. If they offer a NGFW or an encryption solution, that's valuable, but it's just one component of the Zero Trust ecosystem framework. Their capabilities must be market leading as well, meaning that Forrester clients regular shortlist or inquire about the vendor's capabilities and the vendor invests enough in R&D to keep the supporting solutions and feature set competitive (see Figure 3).

› **Create unique technical advantages to solution integration.** A platform vendor must offer more than a portfolio of loosely coupled products and solutions. This could take the form of a unified policy management across solutions in the portfolio like the vendors for NGFW and WSG or it could be integration such as the ability to initiate step-up user authentication based on the detection of unusual user activity in a SUBA or other security analytics solution.

› **Develop and support robust APIs and a partner ecosystem.** Many vendors have broad portfolios, but a portfolio is not necessarily a platform. To be a platform, a vendor must have APIs, SDKs, or events that a developer can build on or integrate with. Most capable players in this space

have open APIs; Cisco, IBM, FireMon, ForcePoint, McAfee, PAN, Symantec, and others have solutions with well-documented APIs that are readily available for development and integration. Additionally, these solutions and their APIs must enable control and management of systems that don't necessarily live in your organization's infrastructure. These tools and systems enable real-time command and control of a wide variety of assets. Security pros should also be concerned with cloud-based workloads, networks, and systems.

› **Maintain a center of gravity for visibility, analysis, policy, and automation.** Not every vendor has a centralized security analytics platform or SIM, but vendors must be able to explain their management vision for reducing the number of point consoles for visibility and analytics, policy management, and, ultimately, automation across their portfolio. There will always be a need for individual product consoles for some elements of implementation and granular configuration, but for overall visibility, policy, and automation and orchestration, a vendor should have a vision, strategy, and road map for reducing the number of consoles to three.

FIGURE 3 Snapshot Of Notable Vendors In The Zero Trust eXtended Ecosystem

Zero Trust platform

- Cisco
- FireMon
- Forcepoint
- Fortinet
- IBM
- iboss
- LogRhythm
- McAfee
- NetFort
- Palo Alto Networks
- RSA
- Securonix
- Sophos
- Trend Micro

Security automation and orchestration

- AWS
- Cisco
- FireMon
- Forcepoint
- Fortinet
- Huawei
- IBM
- iboss
- Juniper
- LogRhythm
- McAfee
- Microsoft
- Palo Alto Networks
- RSA
- Securonix
- Splunk
- Symantec
- Trend Micro

Security visibility and analytics

- AlgoSec
- Cisco
- FireMon
- Forcepoint
- Fortinet
- IBM
- LogRhythm
- McAfee
- NetFort
- Palo Alto Networks
- RSA
- Securonix
- Sophos
- Trend Micro

People: interaction

- Authentic8
- CA Technologies
- Cisco
- Forcepoint
- IBM
- Imperva
- Light Point Security
- McAfee
- Menlo
- Mimecast
- Palo Alto Networks
- Sophos
- Splunk
- Symantec
- Trend Micro
- Zscaler

People: identity

- AWS
- Centrify
- CyberArk
- Gemalto
- IBM
- Microsoft
- Okta
- OneLogin
- Oracle
- Ping Identity
- RSA
- Thycotic

Workload security

- A10 Networks
- AWS
- Barracuda Networks
- Centrify
- CyberArk
- F5 Networks
- ForeScout
- Fortinet
- Huawei
- HyTrust
- IBM
- iboss
- Illumio
- Imperva
- Microsoft
- Oracle
- Palo Alto Networks
- Symantec
- Thales e-Security
- Thycotic
- Trend Micro

Data security

- Boldon James
- Forcepoint
- Gemalto
- Imperva
- IBM
- IONIC Security
- McAfee
- Microsoft
- Sophos
- Spirion
- Symantec
- Thales e-Security
- TITUS
- TokenEx
- Vera Security
- Varonis

Network segmentation

- A10 Networks
- AlgoSec
- AWS
- Barracuda
- Cato Networks
- Check Point
- Cisco
- F5
- FireMon
- Forcepoint
- ForeScout
- Fortinet
- Huawei
- iboss
- Illumio
- Imperva
- Juniper
- NetFort
- Palo Alto Networks
- Portnox
- Sophos
- Trend Micro
- Unisys

Device security

- Centrify
- Check Point
- Cisco
- ForeScout
- Huawei
- IBM
- Juniper
- McAfee
- Microsoft
- MobileIron
- Symantec
- Trend Micro
- VMware AirWatch

Recommendations

Use The ZTX Ecosystem To Set Strategy

Zero Trust has become a critical initiative within the security industry. Security teams across the world in both the government and corporate realms are using the simple but powerful concepts of Zero Trust as the foundation of their strategic plans and road maps.[19] Your security organization should as well. The ZTX ecosystem framework is prescriptive and inclusive of solutions beyond network segmentation. The time to use and progress with a Zero Trust strategic plan is now; to that end we recommend that security leaders:

- **Use the ZTX ecosystem framework to set strategic plans.** We developed our framework to help your team clearly define what it needs to achieve Zero Trust from a technical and operational perspective. This new evolution of the Zero Trust strategy focuses on being more prescriptive but also more inclusive of technologies that help to drive strategic goals. Nothing in this new model and framework exists without a direct correlation of a successful Zero Trust process. Your team should leverage this new evolution as a quantifiable measurement of its evaluation criteria for any strategic plans or vendor POCs. Work to assign specific numeric values to the model and apply those data points to your evaluations; doing this will rack and stack vendor solutions with verifiable data that your team can use to justify the final choice on technology.
- **Make potential vendors detail how they map to the ZTX ecosystem.** Vendors have been preaching the gospel of using Zero Trust technologies for a few years now. In truth, many of them are only offering a piece of the solution set needed to achieve Zero Trust. Use this Zero Trust model and the framework as an evaluation matrix that potential vendors must map to. Your team can directly leverage this model and its inherent criteria to measure all vendors and determine where they would plug into your networks and your strategies. Push potential vendors to provide briefings and presentations on specifically where they align to your Zero Trust strategy and force them to detail where they fall in the model. If those vendors can't answer those questions, then they aren't in alignment with your strategic initiatives.
- **Create a road map that's slow and methodical.** This advice sounds counterintuitive in a world focused on speed and increased adoption of technology, but your team needs to take its time. Speed can be a good thing; however, it's not the best technique to leverage as part of something as in-depth as a strategic move toward achieving Zero Trust. Set your vendor POCs and evaluations to a specific 60-day time frame and use that time to map them to the framework points. Any tooling or capability that can't be quantifiably mapped to the evolved ecosystem is not one you should consider as part of your future Zero Trust initiatives.

Engage With An Analyst

Gain greater confidence in your decisions by working with Forrester thought leaders to apply our research to your specific business and technology initiatives.

Analyst Inquiry

To help you put research into practice, connect with an analyst to discuss your questions in a 30-minute phone session — or opt for a response via email.

Learn more.

Analyst Advisory

Translate research into action by working with an analyst on a specific engagement in the form of custom strategy sessions, workshops, or speeches.

Learn more.

Webinar

Join our online sessions on the latest research affecting your business. Each call includes analyst Q&A and slides and is available on-demand.

Learn more.

Forrester's research apps for iOS and Android.
Stay ahead of your competition no matter where you are.

Endnotes

[1] See the Forrester report "Top Cybersecurity Threats In 2018." Source: Jeff Pollard, "The B2B Breach Trifecta: Equifax, SEC, and Deloitte," Forrester Blogs, September 25, 2017 (https://go.forrester.com/blogs/the-b2b-breach-trifecta-equifax-sec-and-deloitte/).

[2] Source: Heather Somerville and Dan Levine, "Uber lawyer says board, ex-CEO knew of evidence withheld from Waymo case," Reuters, November 30, 2017 (https://www.reuters.com/article/us-alphabet-uber-ruling/uber-lawyer-says-board-ex-ceo-knew-of-evidence-withheld-from-waymo-case-idUSKBN1DT2XT) and Taylor Armerding, "Chinese spies target US intellectual property," CSO Online, August 24, 2015 (https://www.csoonline.com/article/2973542/security-industry/chinese-spies-target-us-intellectual-property.html).

[3] See the Forrester report "The Forrester Wave™: Security Analytics Platforms, Q1 2017."

[4] See the Forrester report "The Eight Business And Security Benefits Of Zero Trust."

[5] See the Forrester report "Future-Proof Your Digital Business With Zero Trust Security."

[6] "Payment security is paramount for every merchant, financial institution, or other entity that stores, processes, or transmits cardholder data. The PCI Data Security Standards help protect the safety of that data." Source: "Maintaining Payment Security," PCI Security Standards Council (https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security).

[7] See the Forrester report "Jump-Start Zero Trust With Forrester's Reference Architecture."

[8] See the Forrester report "Develop Your Zero Trust Workforce Security Strategy" and see the Forrester report "Protect Your Digital Workforce With Browser Isolation Technology (BIT)."

[9] See the Forrester report "Evolve Your IAM Strategy For Your Digital Business."

[10] See the Forrester report "Protect Your Digital Workforce With Browser Isolation Technology (BIT)."

[11] See the Forrester report "The Forrester Tech Tide™: Continuous Deployment Technologies, Q4 2017."

[12] See the Forrester report "Winning In The Age Of The Customer."

[13] See the Forrester report "The IoT Attack Surface Transcends The Digital-Physical Divide."

[14] Source: Alex Schiffer, "How a fish tank helped hack a casino," The Washington Post, July 21, 2017 (https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/).

[15] See the Forrester report "Hardcoded For Failure."

[16] See the Forrester report "Reduce Risk And Improve Security Through Infrastructure Automation."

[17] See the Forrester report "Vendor Landscape: Data Classification, Q3 2017."

[18] We asked 3,752 global security decision makers "Which of the following are the biggest information/IT security challenges for your firm?" Source: Forrester Data Global Business Technographics® Security Survey, 2017.

[19] Source: Cris Thomas, "Zero trust policy the answer to fed cybersecurity challenges," The Hill, September 19, 2016 (http://thehill.com/blogs/congress-blog/technology/296531-zero-trust-policy-the-answer-to-fed-cybersecurity-challenges) and "BeyondCorp: A New Approach to Enterprise Security," Google Cloud Platform (https://cloud.google.com/beyondcorp/).

FORRESTER®
CHALLENGE THINKING. LEAD CHANGE.

We work with business and technology leaders to develop customer-obsessed strategies that drive growth.

PRODUCTS AND SERVICES

- Core research and tools
- Data and analytics
- Peer collaboration
- Analyst engagement
- Consulting
- Events

Forrester's research and insights are tailored to your role and critical business initiatives.

ROLES WE SERVE

Marketing & Strategy Professionals

CMO
B2B Marketing
B2C Marketing
Customer Experience
Customer Insights
eBusiness & Channel Strategy

Technology Management Professionals

CIO
Application Development & Delivery
Enterprise Architecture
Infrastructure & Operations
- Security & Risk

Sourcing & Vendor Management

Technology Industry Professionals

Analyst Relations

CLIENT SUPPORT

For information on hard-copy or electronic reprints, please contact Client Support at +1 866-367-7378, +1 617-613-5730, or clientsupport@forrester.com. We offer quantity discounts and special pricing for academic and nonprofit institutions.